

AFFIDAVIT OF SPECIAL AGENT KEVIN M. McCUSKER

I, Kevin M. McCusker, being duly sworn, hereby depose and state as follows:

1. I am a Special Agent for the Federal Bureau of Investigation (“FBI”) currently assigned to the Boston, Massachusetts Field Office. I have been so employed for over thirteen (13) years. Since August 2011, I have been assigned to the Boston Field Office economic crimes squad. Prior to this assignment, I investigated matters concerning National Security in the Minneapolis and Boston Field Offices. I hold a Bachelor's degree in Accounting and an inactive Certified Public Accountant license. As an FBI Special Agent, I am an investigative or law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7), in that I am empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in 18 U.S.C. § 2516.

2. I am submitting this affidavit in support a criminal complaint charging YANNICK A. MINANG (“MINANG”) with money laundering, in violation of 18 U.S.C. § 1956(a)(1)(B)(i-ii).

3. The facts in this affidavit come from my personal involvement in this investigation, including interviews of witnesses as well as my review of documents and bank records. In submitting this affidavit, I have not included every fact known to me about this investigation. Instead, I have only included facts that I believe are sufficient to establish probable cause.

Background of Investigation

4. The instant investigation targets the participants in a Business Email Compromise (“BEC”) scheme, which appears to work as follows:

a. The BEC scheme begins with the hacking or spoofing of email accounts associated with individuals, businesses, and other entities involved in legitimate business transactions. In some cases, the BEC participants hack into email accounts with stolen passwords and usernames, take over the account, and impersonate the true user. In other cases, the BEC participants “spoof” the victim’s email account by creating a substantially similar email address to impersonate the true user of the account. Thus, the participants of the BEC scheme seek to take over the email accounts of unsuspecting victims, impersonate the actual users of the email accounts, and deceive the recipients of the compromised emails into believing they are communicating with the true owner of the email account.

b. Once the BEC participant impersonates the true owner of the email account, the participant uses the account to deceive other parties in an otherwise legitimate financial transaction and divert funds from the transactions to bank accounts that the scheme participants control. For example, in several instances, a BEC participant has impersonated a party involved in a legitimate real estate transaction, and has used the compromised email to send different wire transfer instructions to divert and misappropriate funds intended for the legitimate transaction.

c. Once the funds are unlawfully misappropriated in this way, the proceeds of the scheme are wired through a series of bank accounts in the United States that the participants in the scheme appear to be using to layer, and thereby conceal, the movement of the funds. Ultimately, a substantial portion of the misappropriated funds are transferred to accounts outside the United States.

5. In recent years, individuals, business entities in public and private sectors, and U.S. financial institutions have become increasingly aware of threat of such BEC fraud schemes

and have notified the FBI about potentially suspect transactions. As further described below, the instant scheme involves accounts that MINANG used at Bank of America and Citizens bank to launder the proceeds of an apparent BEC fraud scheme.

The Current Investigation

6. On or about September 19, 2017, a Bank of America (“BOA”) fraud investigator informed the FBI in Boston about a potential BEC fraud involving a BOA customer living in Massachusetts. According to BOA, the email account of the victim’s real estate broker was compromised and was used to deceive the victim into transferring the proceeds of a real estate transaction to an account under the name “Offre Trading.”

7. According to records from BOA, on or about August 11, 2017, a Massachusetts woman, Eunice Offre, opened the account. Offre is believed to be in an intermittent romantic relationship with MINANG. Days later, on or about August 24, 2017, the BOA Offre Trading account received two wire transfers, each for \$86,000, from the victim of the scheme, who believed he/she was transferring funds to purchase two properties in Nevada.

8. Thereafter, between August 25 and August 28, 2017, approximately \$71,000 was wired from the Offre Trading account to an account in South Africa, and a cashier’s check for approximately \$46,000 was drawn from funds in the Offre Trading account and made payable to “Minang Investments.” This cashier’s check was negotiated at Santander Bank.

9. While investigating the above matter involving the Canadian BEC victim, the FBI learned of another BEC victim in California. As part of this BEC fraud, the California victim was deceived into transferring \$275,250 in closing funds to an account at BOA ending in 7413 (“BOA-7413”) in the name of YANNICK A. MINANG, doing business as (“dba”) “Minang

Trades.” Similar to the first victim, the BEC fraud involved a compromise of the victim’s real estate’s broker email account.

10. The transfer of funds took place on July 3, 2017. MINANG opened this account a short time before, on or about June 22, 2017, with an opening deposit of \$100. The opening deposit and the \$275,250 incoming wire transfer from the California victim are the only credits to BOA-7413 and MINANG was the only authorized signer on the account.

11. Between July 3 and July 6, 2017, MINANG transferred the proceeds of the BEC fraud in the following manner: an international wire transfer of \$137,500 to an account at Standard Bank of South Africa; cashier's checks payable to “Minang Investments” and “C Tah Cho”; and approximately four in-branch cash withdrawals of amounts between \$9,000 and \$9,600, just below the Currency Transaction Reporting requirement of \$10,000.

12. On or about September 22, 2017, SA James Marinelli and I interviewed MINANG at a Panera Bread restaurant in Braintree, Massachusetts. In sum, during the interview, agents asked MINANG about his involvement in large transactions during the summer months of 2017. Concerning the incoming wire of \$275,250 described above, MINANG claimed that he was expecting a loan of \$40,000 from an individual he knew as “Alain” but the amount of money he received was much more, about \$270,000. MINANG claimed that Alain contacted MINANG and advised that the amount MINANG received was too much. Alain then gave MINANG instructions on how to return the excess funds.

13. Also during the interview, MINANG described Offre as an intermittent girlfriend. According to MINANG, an amount in excess of \$100,000 was transferred into Offre’s account because of online ads she had placed for investments in an event planning business she was

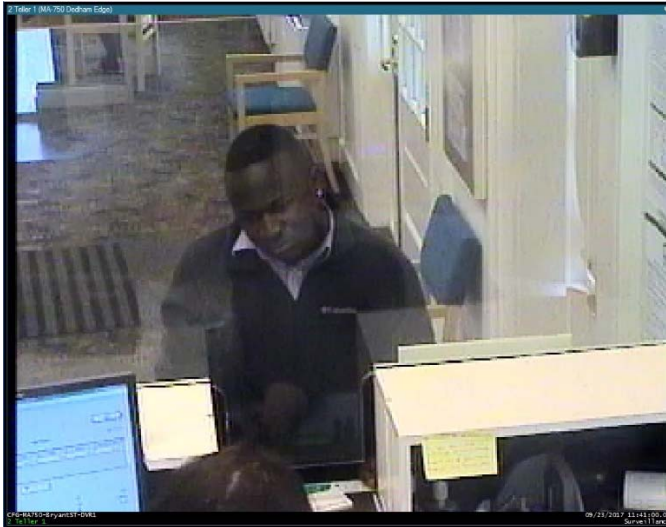
trying to start. MINANG claimed not to know the details regarding the transaction but stated he believed it was similar to circumstances of the funds being transferred to his account.

14. In addition to advising MINANG the importance of telling the truth to federal agents, the interviewing Agents advised MINANG that the funds that had been sent to his and Offre's accounts were the result of fraud, and by receiving the transfers, he was helping launder the proceeds of illegal activity through his account. MINANG was advised to not conduct any further transactions with these funds in his accounts and not to do anything with the remaining funds, including either a withdrawal or wire transfer. Lastly, agents advised MINANG that if he received any additional funds in a similar manner, he should contact the interviewing Agents before doing anything with the funds.

15. On or around September 24, 2017, another California-based victim of BEC filed a complaint on the FBI's online Internet Crime Complaint Center website (IC3.gov). Based on the complaint and my telephonic interview of the victim, I learned that similar to the prior two victims described above, this third victim, on or about September 21, 2017, had been deceived into wiring \$150,000 for a real estate transaction to three different bank accounts. One of the accounts was an account at Citizens Bank ending in 8048 ("CITZ-8048") in the name of "Minang Escrows" with an address of 800 West Street, Braintree, Massachusetts. On or about September 22, 2017, the same day agents interviewed MINANG, CITZ-8048 received a \$30,000 incoming wire transfer from this California-based victim.

16. After the FBI's interview with MINANG, I learned that on Saturday, September 23, 2017, MINANG made two in-branch withdrawals of cash from CITZ-8048. Each withdrawal was below \$10,000, a method used to avoid Currency Transaction Reporting requirements.

17. As further depicted below in the bank surveillance videos, first on September 23, 2017, at approximately 11:41 a.m., MINANG withdrew approximately \$9,000 at branch of Citizens Bank in Dedham, Massachusetts.



18. Second, on September 23, 2017, at approximately 12:47 p.m., MINANG withdrew \$9,500 in cash at a Citizens Bank branch in West Roxbury, Massachusetts.



19. Notably, MINANG withdrew these funds the day after agents informed him of the illegal nature of the scheme and advised him that the type of funds he had been receiving into his accounts were the proceeds of fraud.

Conclusion


20. Based on the foregoing, I submit there is probable cause to believe that YANNICK A. MINANG ("MINANG") has committed the crime of money laundering, in violation of 18 U.S.C. § 1956(a)(1)(B)(i-ii).

Signed under the pains and penalties of perjury this 28th day of September, 2017.



Kevin M. McCusker
Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me this 28th day of September, 2017.



THE HONORABLE M. PAGE KELLEY
UNITED STATES MAGISTRATE JUDGE
DISTRICT OF MASSACHUSETTS